[0071]
(Third Embodiment)
As in the first embodiment, the present embodiment describes a method where the server has a secure printer list and checks after printer authentication whether or not a printer is safe by referring to the list, regarding the form of reference print.

[0072]
FIG. 8 is the configuration diagram of the confidential information printing system in the third embodiment of the present invention. FIG. 9 is the protocol diagram of reference print. FIG. 10 and FIG. 11 are the process flowchart of the printer control unit after the printer with this configuration. FIG. 12 is the process flowchart of the printing data control unit of a server in this configuration.

[0073]
In the configuration of the confidential information printing system in FIG. 8, the same reference numbers are used for the elements same as in FIG. 1 and the description about the same elements is omitted.

[0074]
The process of the printing control unit 301 of the document server 316, the process of the printer control unit 302 of the network printer 317 and the process of the print request unit of the client 318 will be specifically described below.

[0075]
The operation of the embodiment with the above-mentioned configuration is specifically described in operational order. The client 318 generates print request data from a document requested to be printed by a user, a network printer to which the document should be outputted and information for authenticating users who are authorized to print the documents inputted by a user by using the print request unit 305. Documents to be printed and a network printer are specified

in the form of URL/URI on the WEB server.

[0076]
For example, a username and a password can be also used as information for user authentication. Then, the print request unit 305 transmits these print request data to the printer control unit 302 via the cryptocommunication unit 304 and the cryptocommunication unit 303 of the network printer 317.

[0077]
As the process between a client and a printer in this printer control unit 302 is described in a process (a) between a client and a printer in FIG. 10, description is provided in reference to this.

[0078]
At the beginning, printer authentication is performed between a client and a network printer. Printer authentication is performed via the cryptocommunication unit 304 of the client 318 and the cryptocommunication unit 303 of the network printer 317, based on a public key certificate using the printer authentication information 111.

[0079]
The network printer transmits the printer authentication information 111 to a client (S340) and receives an authentication result from the client (S341). If authentication fails (no in S342), the process is terminated. If authentication succeeds (yes in S342), the network printer receives a print request from the client (S 343) and moves on to a process (A) between the server and the printer.

[0080]
Next, the printer control unit 302 transmits the received print request data to the print data control unit 301 of the document server 316 via the cryptocommunication unit 110 and the cryptocommunication unit 107 in the document server to request print data.

[0081]

As the process between a printer and a server in this printer control unit 302 is described in the process (b) between a printer and a server in FIG. 11, description is provide in reference to this.

[0082]
First, printer authentication is performed between a network printer and a document server (S344 and S345).

[0083]
In the present embodiment, it is described that printer authentication is not performed separately, but performed together with server authentication. However, if the elimination of spoofing of a server is not performed, printer authentication can be performed in the form of omitting server authentication.

[0084]
Mutual authentication between a server and a printer is performed via the cryptocommunication unit 107 of the document server 316 and the cryptocommunication unit 107 of the network printer 317 through mutual authentication based on a public key certificate using the server authentication information 104 and the printer authentication information 111. See references listed in "Conventional technologies" for more details.

[0085]
Also, although the cryptocommunication unit 107, 110, 303 and 304 are not specified in the above-mentioned description, in the case that TCP/IP communication is performed by using known technology such as SSL and TLS, the process of the printer control unit 302 and the process of the print data control unit 301 can be omitted because in SSL/TLS, server authentication (in this case, a network printer in the printer authentication of a client, and a document server in the printer/server mutual authentication) can be performed and client authentication (in this case, a network printer) can be performed as an option before cryptocommunication is performed.

[0086]
The network printer terminates a process if mutual authentication between a server and a printer fails (no in S346). If mutual authentication between a server and a printer succeeds (yes in S346), the network printer requests print data by transmitting print request data to the document server (S347). Subsequently, the network printer receives a user authentication result from the document server (S348) and if the user authentication fails (no in S349), the process is terminated. If the user authentication succeeds (yes in S349), the network printer receives print data (S350) and transmits the print data to the printing unit 113 (S351). After printing is completed, the network printer gives the notice of the completion of printing to the client (S352) and terminates the process.

[0087]
Also, since a process in the printing data control unit 301 is described in the process flowchart of the printing data control unit in FIG. 12, description is provided in reference to this.

[0088]
Receiving a printing data request from the network printer, the document server performs the above-mentioned mutual authentication between a server and a printer (S320). If mutual authentication between the server and the printer fails to succeed (no in S321), the printing data control unit 301 gives the notice of print rejection to a client via the printer (S329) and terminates the process. If mutual authentication between the server and the printer succeeds (yes in S321), the printing data control 301 extracts a URI of the target network printer from the print request data and checks it based on the secure printer list 102 (S322). If the network printer is not included in a list of printers which is authorized to output the document (no in S323), the notice of print rejection is given to a client via the printer (S330) and the process is terminated. If the network printer is included in a list of printers which is authorized to output the document (yes in S323), the printing data control unit 301 extracts the document URI and the user authentication information from the print request data

(S324). Subsequently, the printing data control unit 301 performs user authentication based on user authentication information and checks the user list 103 including users with printing authority and usernames to confirm if the user is authorized to print the document. If user authentication fails or the user is judged to have no printing authority (no in S326), the notice of print rejection is given to a client via a printer (S331) and the process is terminated. If user authentication and printing authority are confirmed (yes in S326), print data is transmitted to the network printer (S327) and the notice of normal termination is given (S328) and the process is terminated.

[0089]
The mutual communication protocol between the above-mentioned client, document server and network printer is shown in FIG. 9 and description is provided as follows:

[0090]
First, a client performs printer authentication on a network printer. If the printer authentication succeeds, the client transmits user authentication information inputted by the document URI and a user as print request data to the network printer. Mutual authentication is performed between the network printer and the network server and if the authentication fails (NG), the notice of print rejection is given to the client via the printer and the process is terminated. If authentication succeeds (OK), the network printer requests print data from the document server. The document server performs user authentication based on the received user authentication information and if user authentication fails (response, NG), the notice of print rejection is given to the client via the printer and the process is terminated. If user authentication succeeds (OK), the document server transmits print data to the network printer. The network printer prints the received print data, and after printing is completed, it gives a print completion notice (response (success)) to the client and the process is terminated.

[0091]
As mentioned above, performing authentication based on public key

certificate and checking based on the list of printers registered as secure printers would avoid output to inappropriate printers.

[0092]
(Fourth Embodiment)
In the present embodiment, measures against the piracy of user authentication information, which can occur in the form of reference print, is described.

[0093]
FIG. 13 is a configuration diagram of the confidential information print system in the fourth embodiment of the present invention. In the print data control unit 501 of the document server 516, the process contents are a modification of the process contents in the print data control unit of the third embodiment in the form of reference print in FIG. 8. The modified process contents are described in the process flowchart of the print data control unit in FIG. 15.

[0094]
The print request data encryption unit 502 and the print request unit 503 in the client 518 perform processes inherent to the present embodiment and the process contents is described below.

[0095]
As 101, 102, 103, 104, 106 and 107 in the document server 516 and 110, 111, and 113 in the network printer 517 are the same reference numbers used for the elements same as in FIG. 1 as well as 302 and 303 in the network printer 517 and 304 in the client 518 are the same as the number elements of FIG. 8, description is omitted.

[0096]
Secondly, the operation of the embodiment with the above-mentioned configuration is specifically described focusing on the difference from the third embodiment. As described above, since in the reference print form, user authentication information should be always transmitted to the document server via the network printer, there is a risk such as

re-obtaining a document by reusing user authentication information obtained through the spoofing of the network printer and eavesdropping on the data transmission channel as well as the diversion of user authentication information to access other documents.

[0097]
To deal with this, when generating print request data by using the print request unit 503, the client 518 of the present embodiment encrypts using the print request data encryption unit 502 at least part of the print request data to allow its decryption only by the document server.

[0098]
The methods of this encryption include encryption by using a public key (which should be obtained in advance or can be obtained by connecting to the document server by the above-mentioned SSL/TLS at this time) included in the public key certificate of the document server. As it is widely known, this method uses the nature that data encrypted by a specific public key can be decrypted only by a secret key corresponding to its public key, while data encrypted by the public key of the document server can be decrypted only by a secret key that is reserved by the document server alone.

[0099]
As print request data to be encrypted, if the user authentication method uses a username and a password, at least the password should be encrypted. It is also effective to include the document URI to prevent the diversion of this print request data to access to other documents as well as to include the printer URI to prevent access from other network printers.

[0100]
Moreover, to prevent multiple printing by a spoofing network printer which repeatedly uses the same print request data, it is effective to add to specific print request data, data such as the generation time data of print request data, the serial number and the random number to be

distinguished from other data and encrypt the resulting data. The example of encrypted print data is shown in FIG. 16.

[0101]
Although print request data generated by the print request unit 503 is transmitted to the document server 516 via the network printer 517, in the process of the network printer 517, part of print request data to be transmitted along with the print data request of step S347 of FIG. 11 is only encrypted and the process is not changed. The reference print protocol (5) in FIG. 14 shows how encrypted user authentication information is transmitted.

[0102]
Subsequently, the process in the document server 516 is described in reference to the process flowchart of the print data control unit in FIG. 15. The difference between FIG. 15 and FIG. 12 of the third embodiment is, in step S524 (S324 in FIG. 12), necessary data extracted after the decryption of print request data which is at least partly encrypted in the client 518, using a secret key of the document server which is stored only in the document server as part of the server authentication information 104.

[0103]
At this point, if the above-mentioned document URI, printer URI and print request generation time are included in print request data, the piracy and diversion of print request data can be prevented by comparing a printer which requests print data and the printer URI as well as comparing a document requested to be printed and the document URI. Also, print request data can be controlled to be valid only for a predetermined short time period in the document server, or data such as print request generation time and the serial number which are available for distinguishing a predetermined print request data can be used to prevent the multiple use of the same print request data by a spoofing network printer.

[0104]

As described above, according to the present embodiment, the piracy and reuse of user authentication information which can occur in the form of reference print can be prevented and only a valid user authorized to print the document is allowed to print the document to a secure printer in accordance with the authentication of the network printer and the confirmation of secure printers.

[0105]
(Fifth Embodiment)
In the present embodiment, as countermeasures against the piracy of user authentication information which can occur in the form of reference print, a method of using the public key certificate of a user is described.

[0106]
FIG. 17 is a configuration diagram of confidential information printing system in the fifth embodiment in the present invention. In the figure, the print data control unit 602 in the document server 616 is the modification of the process content of the print data control unit 501 in the fourth embodiment in the form of reference print of FIG. 13. The modified process content is included in the process flowchart of the print data control unit of FIG. 19.

[0107]
The list 601 of classes with printing authority can replace the list 103 of users with print authority in FIG. 13. Its content and usage are described below.

[0108]
Also, the user authentication expansion information 603 stored in the memory unit 605 in the client 618 and the print request unit 604 are directed to processes unique to the present embodiment. Its content is described below. Moreover, the print request data encryption unit 502 is the same as the element assigned the same number of FIG. 13.

[0109]

101, 102, 104, 106 and 107 in the document server 616 and 110, 111 and 113 in the network printer 617 are the same as the element assigned the same number of FIG. 1 as well as 302 and 303 in the network printer 617 and 304 in the client 618 are the same as the element assigned the same number of FIG. 8. Therefore, the description is omitted.

[0110]
Subsequently, the operation of the embodiment with the above-mentioned configuration is specifically described focusing on difference from the fourth embodiment. Although in the fourth embodiment, the case that the user authentication method uses a username and a password is described, in the present embodiment, the case that the user authentication method is employed based on a user's public key certificate is described.

[0111]
After the print request unit 604 of the client 618 receives the input of print request data such as the document URI to be printed and the network printer URI to be outputted, the print request unit 604 of the client 618 generates a digital signature for part of or all of the print request data, or their respective digest information by using a secret key corresponding to a public key certificate included in the user authentication expansion information 603. (This digital signature proves that print request data included in a print request in the document server 616 is not tampered when checking such print request data) The print request unit 604 of the client 618 regards the print request data with this digital signature as new print request data and encrypts the data by a public key of the document server through the print request data encryption unit 502 as done in the fourth embodiment, and then transmits the data to the document server 616 via the network printer 617.

[0112]
If the user authentication of the document server is not performed through directory services such as LDAP and the public key certificate of

a user cannot be available, a digital signature and the user's public key certificate itself should be added to the above-mentioned print request data. The example of print request data and a digital signature is shown in FIG. 20.

[0113]
As in the fourth embodiment, the process in the network printer 617 is not changed except that the print request data format to be transmitted when requesting print data (in step S347 in FIG.11 of the third embodiment that was referred to in the fourth embodiment) is different from that of the fourth embodiment. The reference print protocol (6) in FIG.18 shows how the encrypted user authentication expansion information is transmitted.

[0114]
The document server 616 which receives a print request via the network printer 617 performs processes through the print data control unit 602. The content of the processes are shown in the process flowchart of the print data control unit in FIG. 19 and is different from the process content of the print data control unit 501 in the fourth embodiment in terms of user authentication in S622, the branch S623, the print rejection notice due to authentication failure S631 and the confirmation of print authorization in S624 and S625.

[0115]
First, user authentication is performed in S622. User authentication is performed by confirming that the digital signature is valid. Data to be provided with digital signatures such as the document URI and the printer URI, which are generated in the print request unit 604 of the client 618, are extracted from print request data decrypted by the public key of the server (or if digest information is used, digest information should be created). Then, these data are checked with the public key of a user about if these data correspond to digital signatures extracted from decrypted print request data in the same way (S622).

[0116]

Here, the public key of a user can be extracted from directory services such as LDAP if the services are used for the user authentication of the document server. If this is not the case, the public key can be extracted from a user public key certificate attached to the above-mentioned print request data with digital signatures. If a digital signature does not correspond to its target data and authentication fails (no in S623), the notice of print rejection is given (authentication failure) (S631) and the process is terminated. If authentication succeeds (yes in S623), the process moves on to the checking of print authorization for the documents in S 624 and S 625.

[0117]
In the fourth embodiment, the confirmation of document printing authority is performed through the checking based on the list of users with printing authority related to the document. However, the present embodiment uses the method of using a predetermined user class described in the expansion part of a user public key certificate. Here it is assumed that a class name related to the document access authority is described in the expansion part of a user public key certificate included in the user authentication expansion information 603 in the client 618. If this class name meets the list 601 of classes that authorizes printing related to documents, it is regarded to have printing authority. Access-authority related class names include office organizations and official responsibility.

[0118]
FIG. 21 shows an example of a user public key certificate with an expansion part issued by an organization which a user belongs to. In this example, the user is identified as the general manager class and user authentication succeeds on confidential information that authorizes printing by general managers and upper management in the document server.

[0119]
In step S 624, the expansion part of a user public key certificate transmitted as print request data is extracted to obtain a class name

related to the user access authority. Subsequently, in step S 625, this information is checked based on the list 601 of classes with printing authority in the document server 616 and the printing authority is confirmed. The following processes are the same as those in the fourth embodiment.

[0120]
The merit of this method is that because printing authority is assigned to a user class rather than a user name itself, the list of classes that is authorized to perform printing related to documents can be easily controlled.

[0121]
As described above, according to the present embodiment, the encryption of print request data by the public key of the document server as well as authentication using a user public key certificate and a digital signature make it possible to further reduce the risk of counterfeiting and diversion of print request data, preventing piracy and reuse of user authentication information which might occur in the form of reference print. Also, through the authentication of network printers and the confirmation of secure printers, only valid users with the printing authority of the documents can perform printing to secure printers.

[0122]
The print request unit 604 in the client 618 encrypts and transmits print request data with a digital signature by the public key of the document server through the print request data encryption unit 502. Unlike the example of the fourth embodiment, however, in the present embodiment, since digital signatures are added to print request data, counterfeiting is considered to be difficult. Therefore, as preventing the decryption of print request data by a spoofing network printer is not always necessary, the encryption of print request data by the public key of the document server in the client and the decryption process in the document server can be omitted.

[0123]

Also, the method of preventing piracy and reuse of print request data (or user authentication information) shown in the fourth embodiment and the fifth embodiment makes it possible to combine the confirmation of secure printers shown in the second embodiment and the usage of secure classes corresponding to documents. This combination can help achieve the goal in which only valid users with the printing authority of the documents can perform printing to secure printers.

[0124]
As mentioned above, prior to printing, the authentication of a network printer is performed and the printer to be confirmed as valid need to be checked if there is the print authorization of the document. To this end, the public key certificate which can identify the printer and its corresponding secret key is provided in the network printer and the authentication of the printer based on the public key certificate is performed before the transmission of the document data. Moreover, the list of secure network printers corresponding to the appropriate classification of documents is provided in the document server, and then the authenticated network printer is checked based on the list. Consequently, the above-mentioned issues can be resolved.

[0125]
Prior to the transmission of document data, the authentication of a network printer based on its public key certificate and the security confirmation of a printer corresponding to the appropriate classification of documents make it possible to prevent the spoofing of a network printer and perform printing to only secure printers.

[0126]
Also, the user client encrypts and transmits at least part of print request data including user authentication, which can be decrypted only by the document server. Then the document server which receives the partly-encrypted print request data via the network printer checks if the print request is counterfeit when checking the printing authority of the user of the document. This can prevent the piracy of information indicating user authentication and printing as well as the reuse of

documents and diversion to the access of other documents.

[0127]
In the system of printing documents including confidentiality controlled in the document server to a printer connected to the network, reuse or the piracy of user authentication information that might occur in the form of reference print can be prevented. Also, the authentication of network printers and the confirmation of secure printers allow only valid users with printing authority for the printing of the documents to print to the secure printers.

[0128]
The present embodiment can be realized by executing a program. Also, the method of providing a program to a computer can be applied as the embodiment example of the present invention. Such methods include media such as CD-ROM recorded with such program and transmission media such as the internet via which a program can be transmitted. The above-mentioned program, media and transmission media are in the category of the present invention.

[0129]
The above-mentioned embodiments show only small examples in the embodiment of the present invention and the range of technology in the present invention should not be interpreted in a limited way because of these embodiments. In other words, the present invention can be embodied in a variety of forms without deviating from its technical idea and main features.

FIG. 8

101 Memory unit
102 List of secure printers
103 List of users with printing authority
104 Server authentication information
106 Document storage unit
107 Cryptocommunication unit
301 Print data control unit
316 Document server

110 Cryptocommunication unit
111 Memory unit
Printer authentication information
302 Printer control method
303 Cryptocommunication unit
113 Printing unit
317 Network printer

304 Cryptocommunication unit
305 Print request unit
318 Client

【図8】

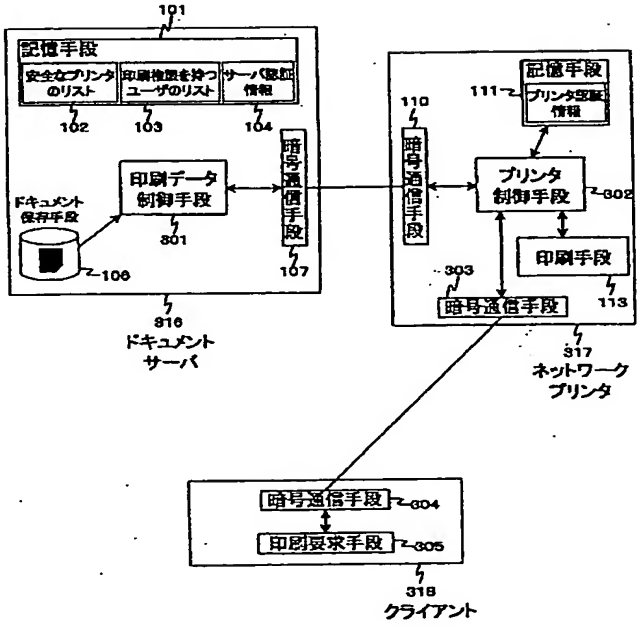


FIG. 9

【図9】

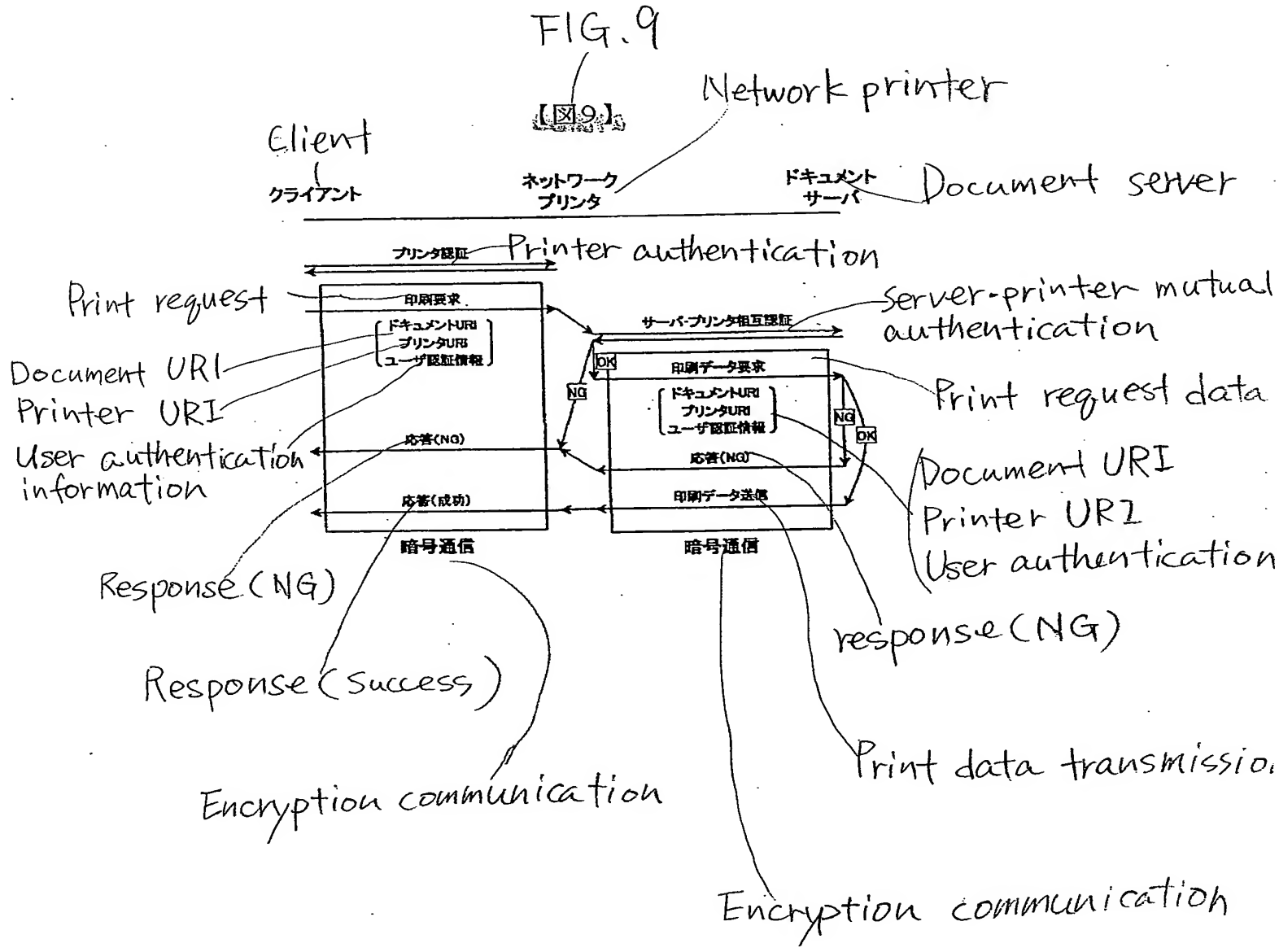
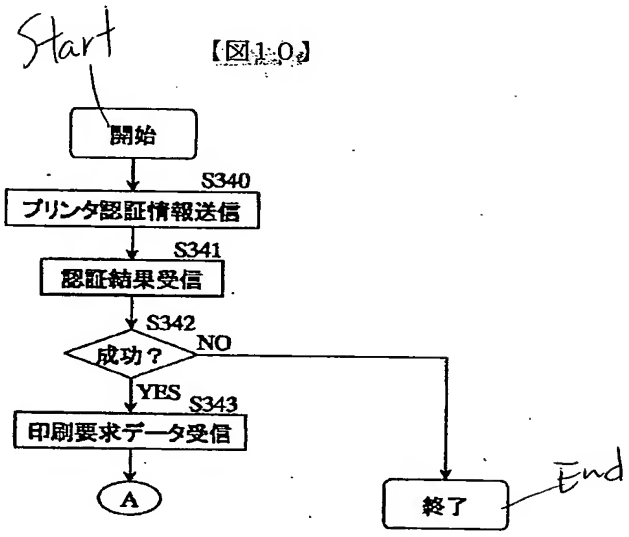

Client
クライアント
Network printer
ネットワークプリンタ
ドキュメントサーバ
Document server
プリンタ認証
Printer authentication
Print request
印刷要求
ドキュメントURI
プリンタURI
ユーザ認証情報
Document URI
Printer URI
User authentication information
応答(NG)
応答(成功)
暗号通信
Response (NG)
Response (Success)
Encryption communication
サーバ・プリンタ相互認証
Server-printer mutual authentication
OK
NG
印刷データ要求
Print request data
Document URI
Printer URI
User authentication
response (NG)
印刷データ送信
Print data transmissio
Encryption communication

FIG. 10
S340 Printer authentication information transmission
S341 Authentication result receiving
S342 Success?
S343 Print request data receiving



クライアント-プリンタ間の処理

Process between client and printer

FIG. 11

S344 Mutual authentication between server and printer

S345 Authentication result receiving

S346 Success?

S347 Print data request

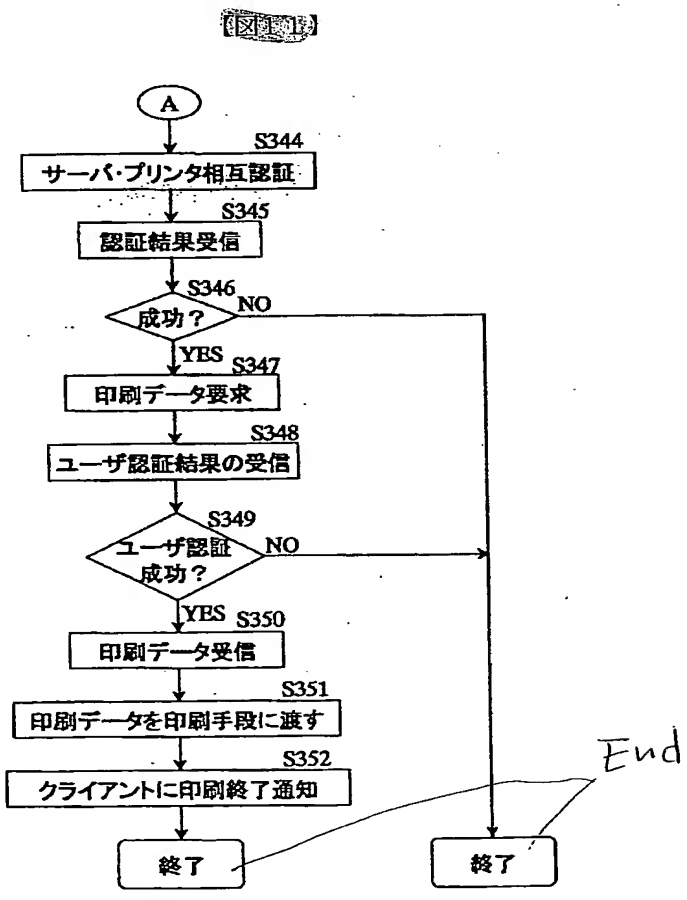
S348 User authentication result receiving

S349 User authentication success?

S350 Print data receiving

S351 Transmit print data to printing unit

S352 Print termination notice to client



プリンタ・サーバ間の処理

Process between client and printer

FIG. 12

S320 Mutual authentication between server and printer

S329 Print rejection notice (authentication failure)

S322 Check a printer which requests print data based on the secure printer list

S330 Print rejection notice (unsecured printer)

S324 Extract document URI and user authentication information from print data request

S325 Check based on the list of users with printing authority and confirm printing authority

S331 Print rejection notice (no print right)

S327 Print data transmission

S328 Normal termination notice

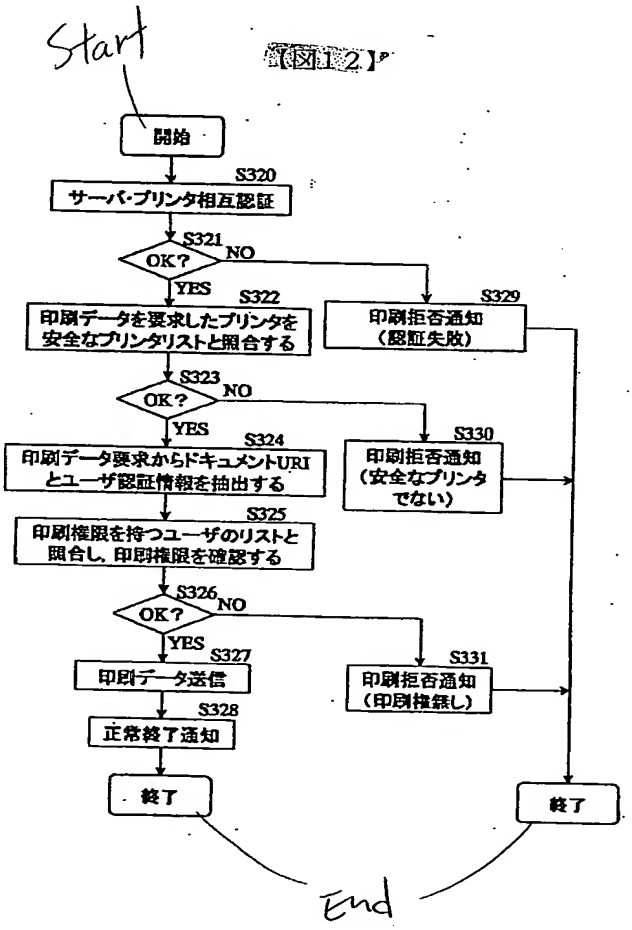


FIG. 13
101 Memory unit
102 List of secure printers
103 List of users with printing authority
104 Server authentication information
106 Document storage unit
501 Print data control unit
107 Cryptocommunication unit
516 Document server

110 Cryptocommunication unit
111 Memory unit
Printer authentication information
302 Printer control method
303 Cryptocommunication unit
113 Printing unit
517 Network printer

502Print request data encryption unit
304 Cryptocommunication unit
503 Print request unit
518 Client

【図13】

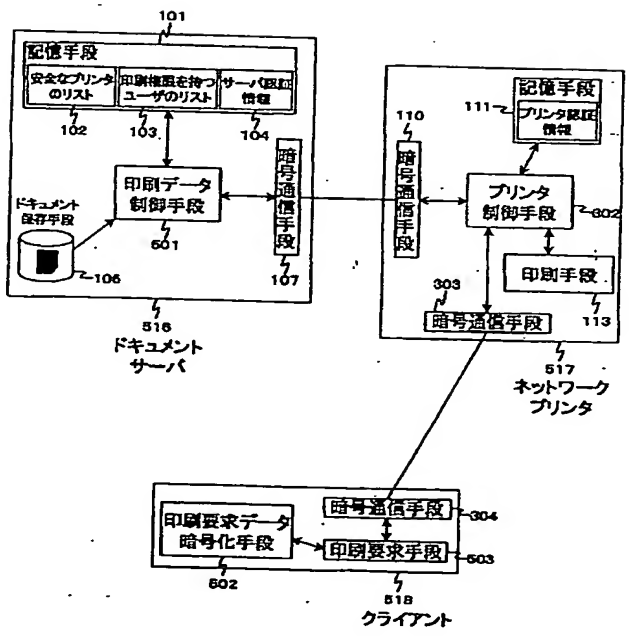


FIG. 14

【図14】

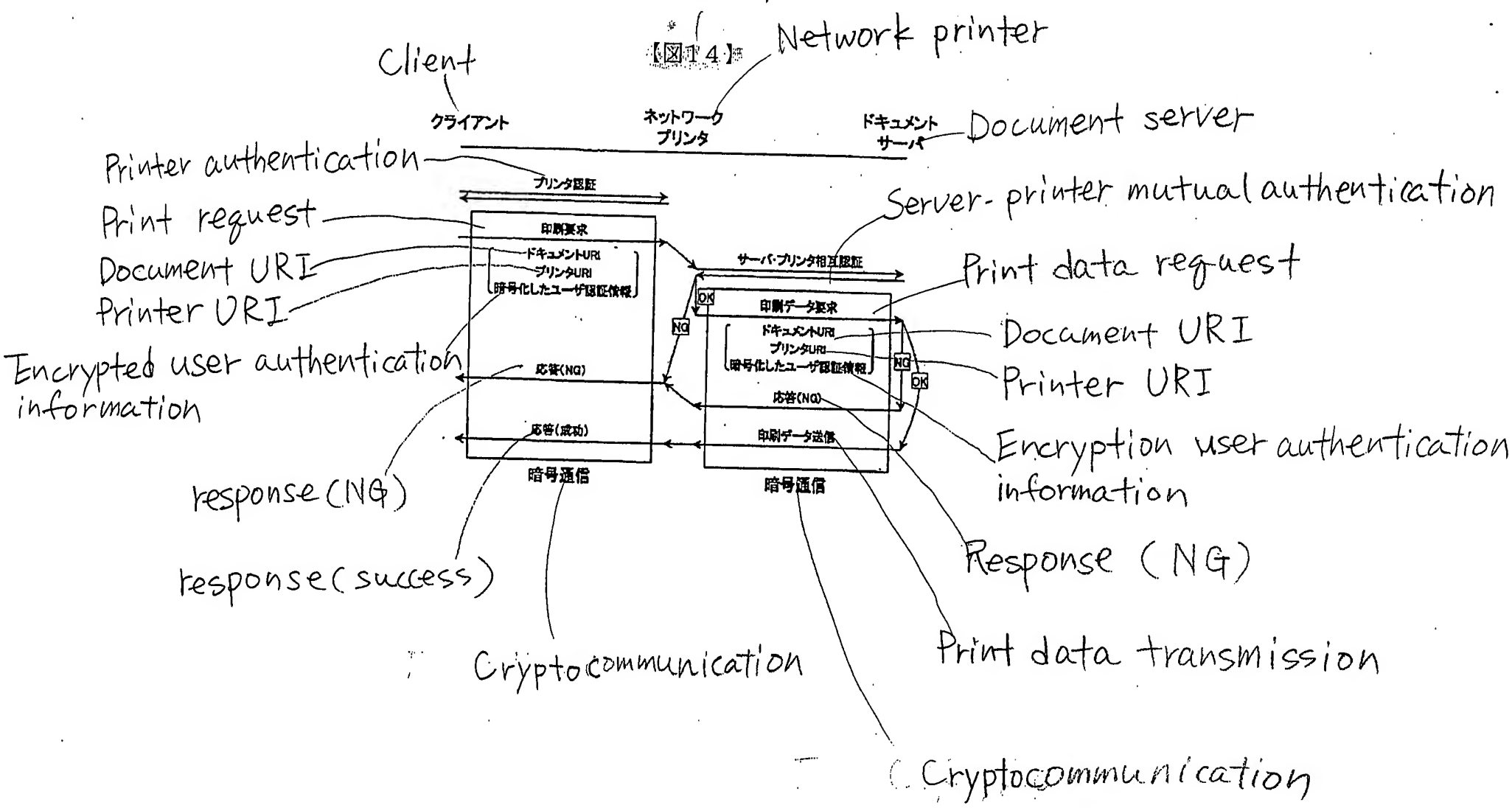

Client
Network printer
クライアント
ネットワークプリンタ
ドキュメントサーバ
Document server
Printer authentication
プリンタ認証
Print request
印刷要求
Document URI
ドキュメントURI
Printer URI
プリンタURI
暗号化したユーザ認証情報
Encrypted user authentication information
応答(NG)
response(NG)
応答(成功)
response(success)
暗号通信
Cryptocommunication
Server-printer mutual authentication
サーバ・プリンタ相互認証
OK
NG
Print data request
印刷データ要求
Document URI
Printer URI
Encryption user authentication information
Response (NG)
印刷データ送信
Print data transmission
Cryptocommunication

FIG. 15

S320 Mutual authentication between server and printer

S329 Print rejection notice (authentication failure)

S322 Check a printer which requests print data based on the secure printer list

S330 Print rejection notice (unsecured printer)

S524 Decrypt encrypted print request data and extract document URI and user authentication information

S325 Check based on the list of users with printing authority and confirm printing authority

S331 Print rejection notice (no print right)

S327 Print data transmission

S328 Normal termination notice

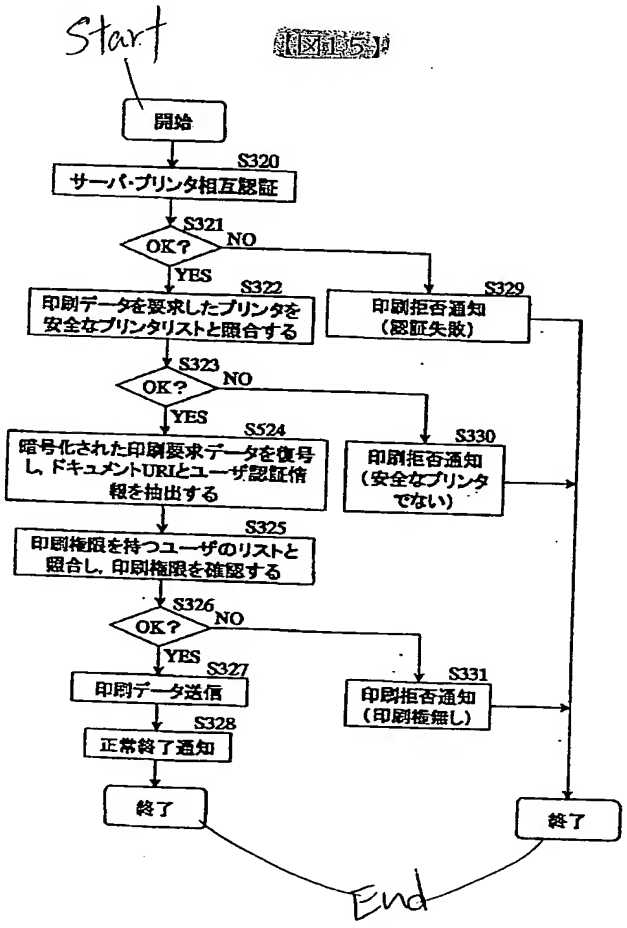


FIG.16

【図16】

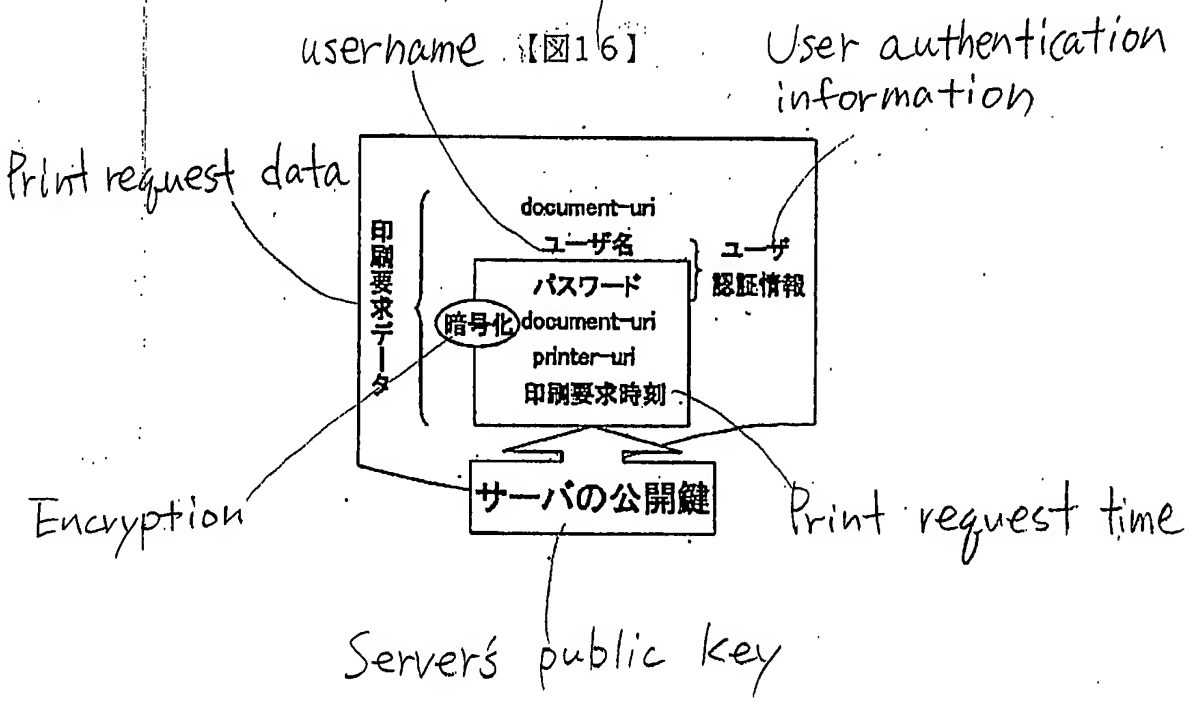

username
User authentication information
Print request data
印刷要求データ
document-uri
ユーザ名
パスワード
暗号化
document-uri
printer-uri
印刷要求時刻
ユーザ認証情報
サーバの公開鍵
Encryption
Print request time
Server's public key

FIG. 17

101 Memory unit
102 List of secure printers
103 List of users with printing authority
104 Server authentication information
106 Document storage unit
602 Print data control unit
107 Cryptocommunication unit
616 Document server

110 Cryptocommunication unit
111 Memory unit
Printer authentication information
302 Printer control method
303 Cryptocommunication unit
113 Printing unit
617 Network printer

502Print request data encryption unit
605 Memory unit
603 User authentication expansion information
304 Cryptocommunication unit
503 Print request unit
618 Client

【図17】

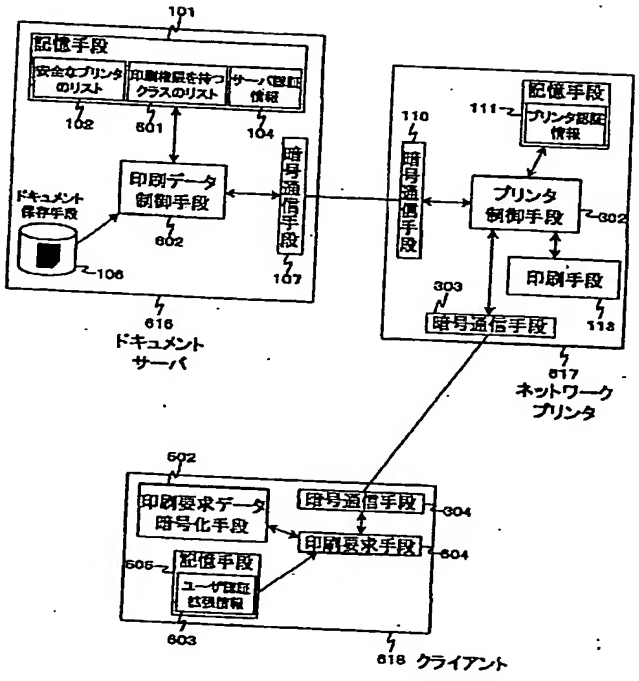


FIG. 18

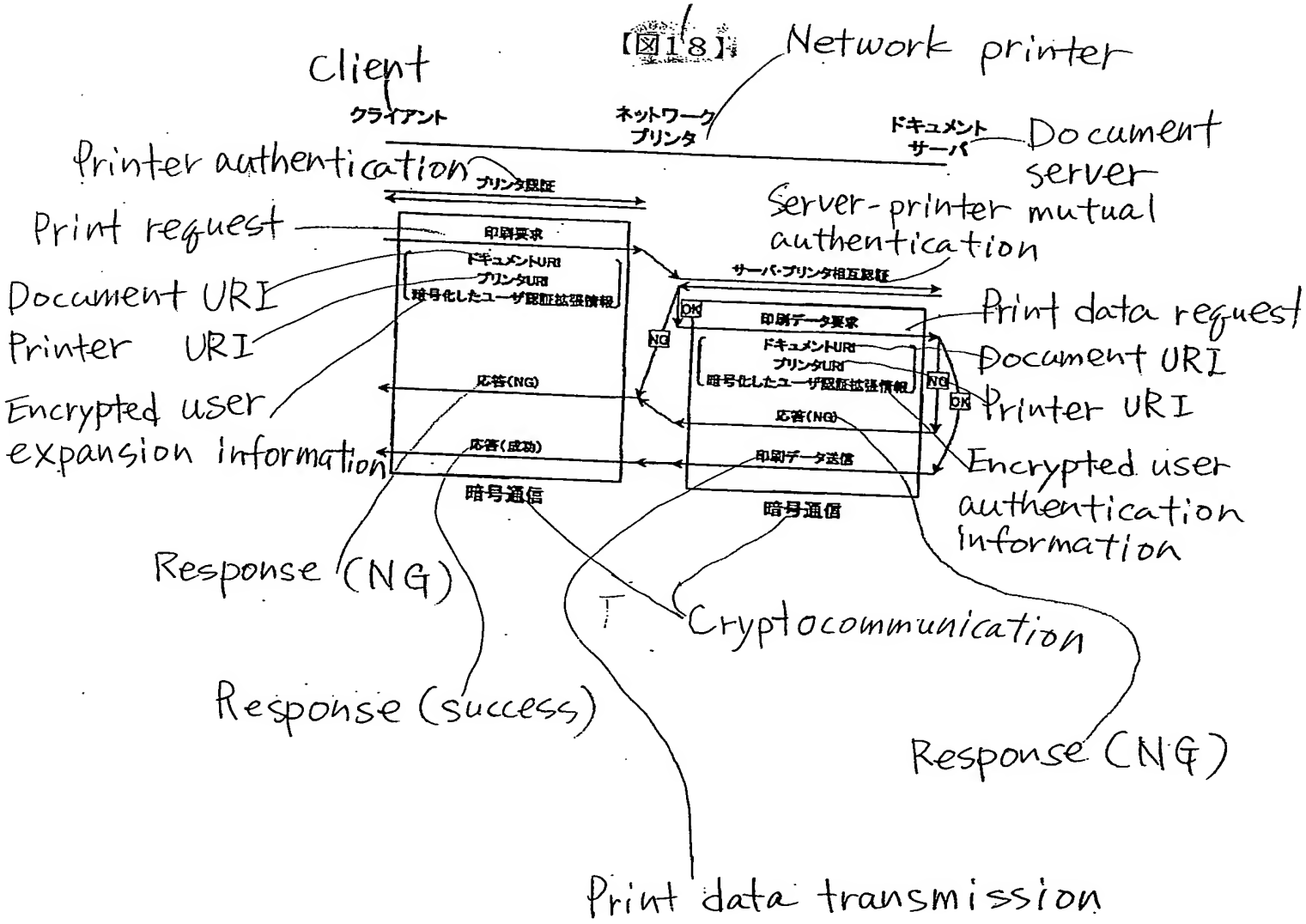

[図18]
Client
クライアント
Network printer
ネットワークプリンタ
ドキュメントサーバ
Document server
Printer authentication
プリンタ認証
Print request
印刷要求
Document URI
Printer URI
Encrypted user expansion information
ドキュメントURI
プリンタURI
暗号化したユーザ認証拡張情報
Server-printer mutual authentication
サーバ・プリンタ相互認証
OK
NG
印刷データ要求
Print data request
Document URI
Printer URI
Encrypted user authentication information
応答(NG)
応答(成功)
印刷データ送信
暗号通信
Response (NG)
Response (success)
Cryptocommunication
Print data transmission

FIG. 19

S320 Mutual authentication between server and printer

S322 Check a printer which requests print data based on the list of secure printers

S329 Print rejection notice (authentication failure)

S330 Print rejection notice (unsecured printer)

S524 Decrypt encrypted print request data and extract document URI and user authentication information

S622 User authentication

S631 Print rejection notice (authentication failure)

S625 Check based on the list of users with printing authority and confirm printing authority

S331 Print rejection notice (no print right)

S327 Print data transmission

S328 Normal termination notice

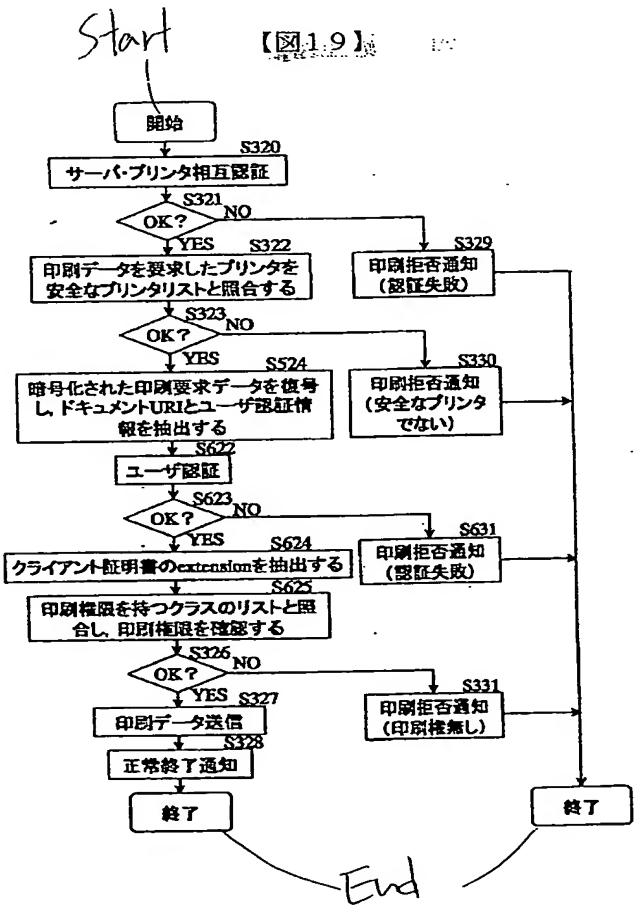


FIG. 20

【図20】

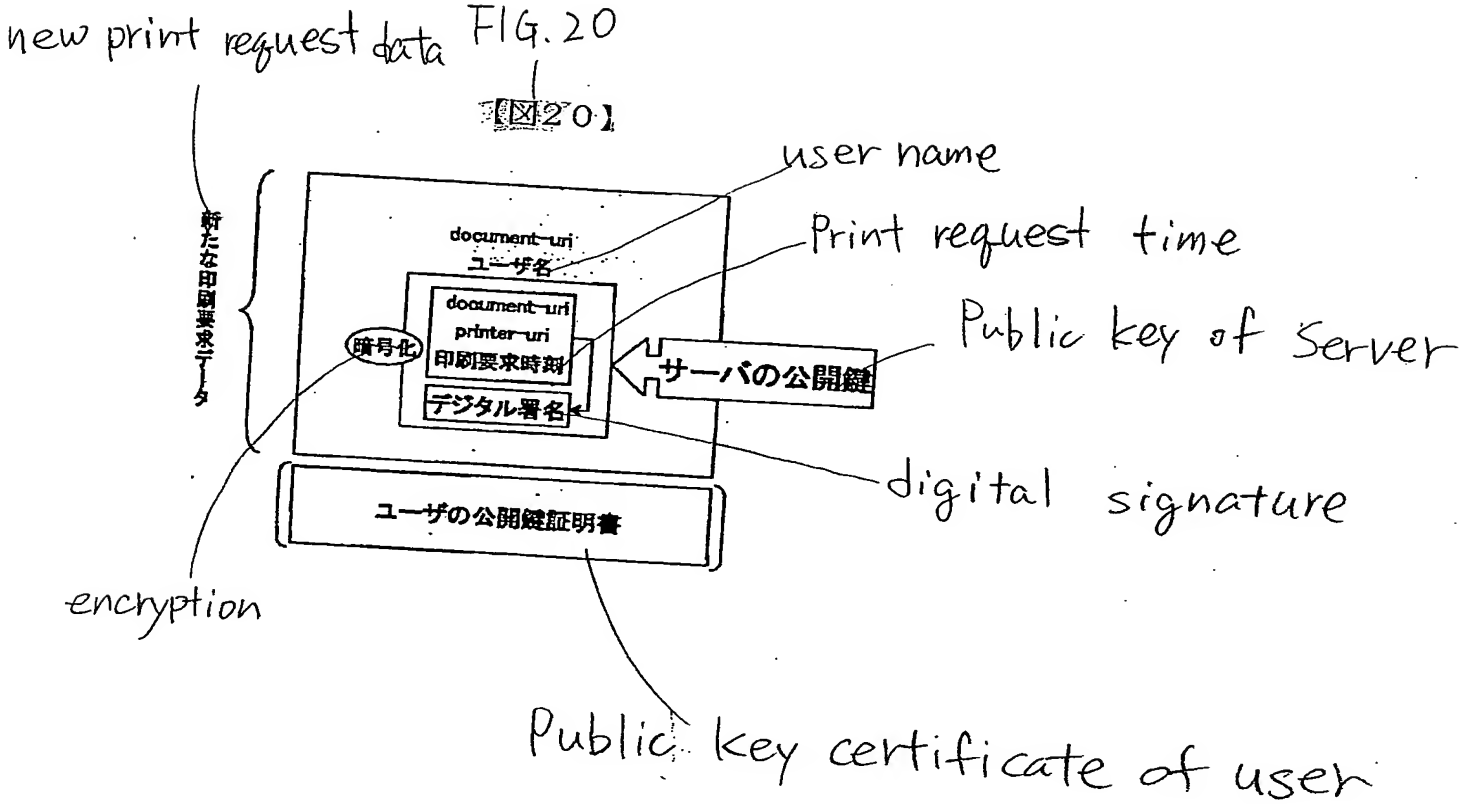

新たな印刷要求データ
document_uri
ユーザ名
document_uri
printer_uri
印刷要求時刻
暗号化
サーバの公開鍵
デジタル署名
ユーザの公開鍵証明書
new print request data
user name
Print request time
Public key of Server
digital signature
encryption
Public key certificate of user

FIG.21

【図21】

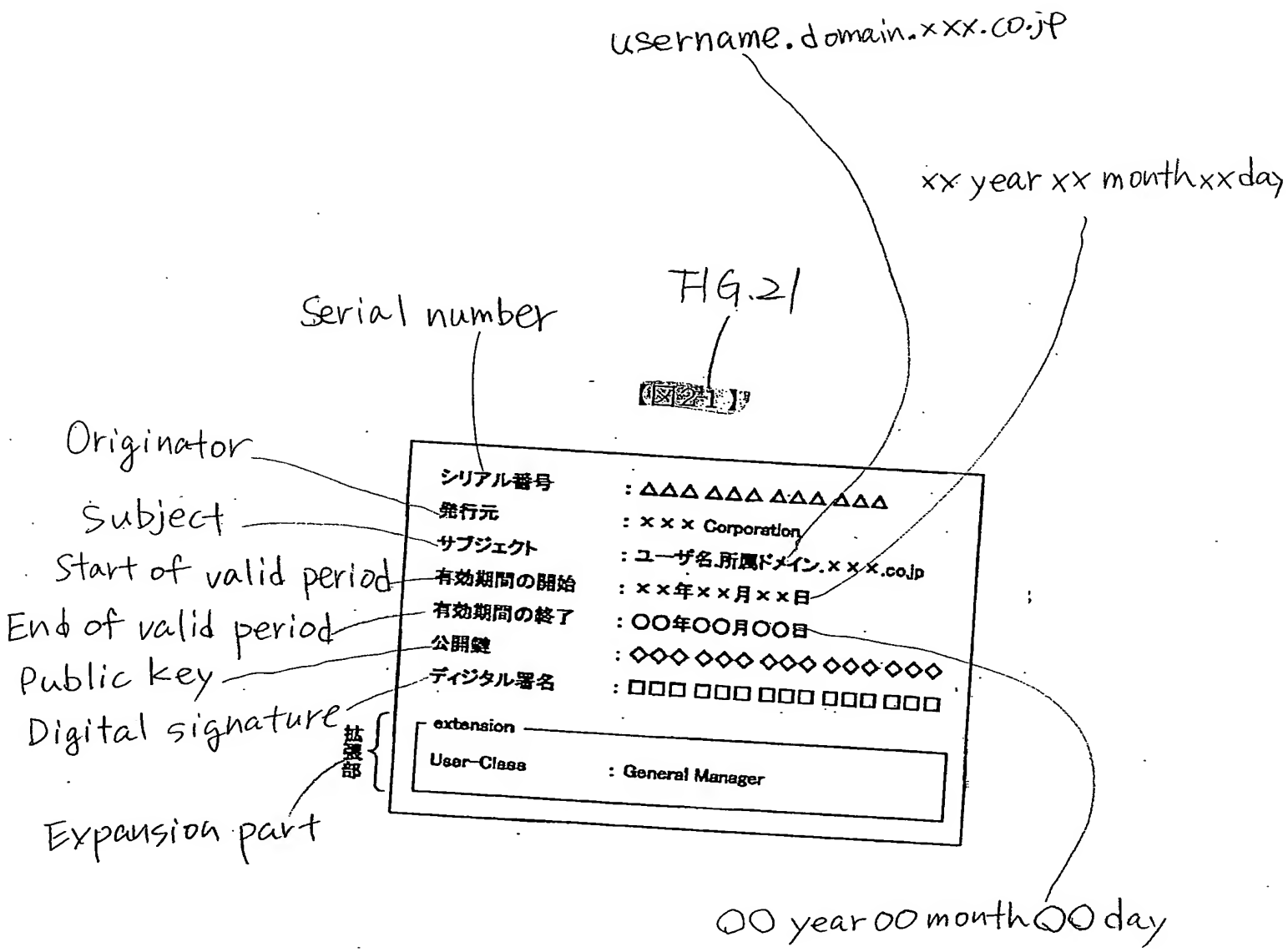
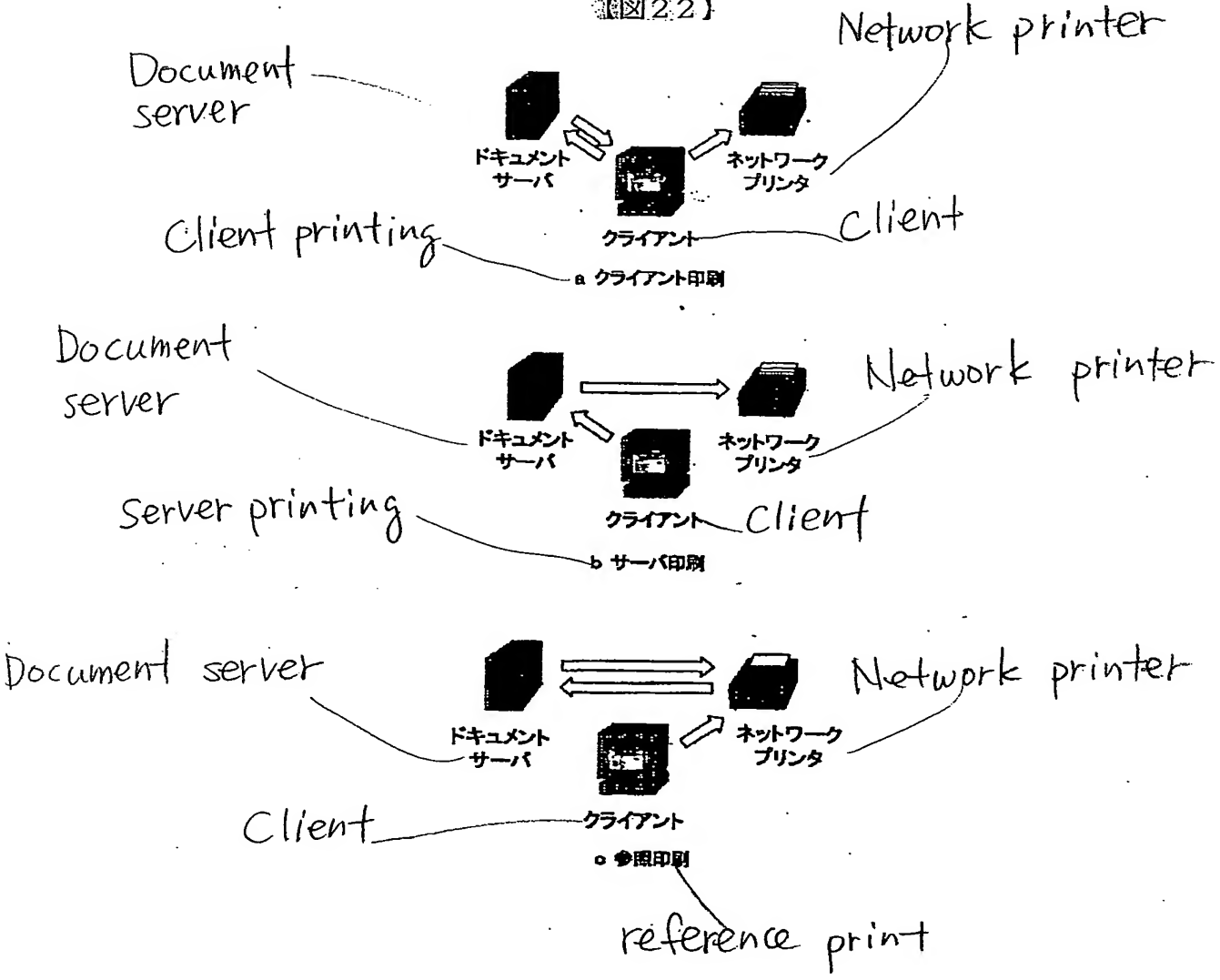

username.domain.xxx.co.jp
xx year xx month xx day
Serial number
Originator
Subject
Start of valid period
End of valid period
Public key
Digital signature
Expansion part
シリアル番号 : △△△ △△△ △△△△△△
発行元 : ××× Corporation
サブジェクト : ユーザ名.所属ドメイン.×××.co.jp
有効期間の開始 : ××年××月××日
有効期間の終了 : ○○年○○月○○日
公開鍵 : ◇◇◇ ◇◇◇ ◇◇◇ ◇◇◇ ◇◇◇
ディジタル署名 : □□□ □□□ □□□ □□□ □□□
拡張部
extension
User-Class : General Manager
○○ year ○○ month ○○ day

FIG.22

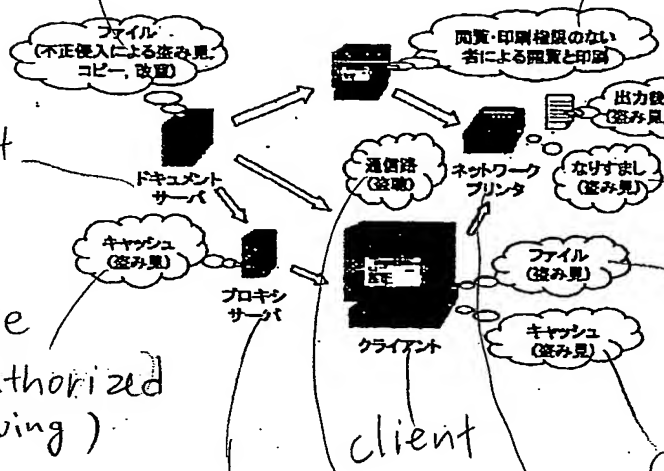
【図22】


Document server
Network printer
ドキュメントサーバ
ネットワークプリンタ
クライアント
Client printing
Client
a クライアント印刷
Document server
Network printer
ドキュメントサーバ
ネットワークプリンタ
クライアント
Server printing
Client
b サーバ印刷
Document server
Network printer
ドキュメントサーバ
ネットワークプリンタ
Client
クライアント
c 参照印刷
reference print

File (unauthorized viewing, copying and tempering due to hacking)

FIG. 23

【図23】



Browsing and printing by someone who has no browsing and printing authority

Outputted document (unauthorized viewing and copying

Document server

Spoofing (unauthorized viewing)

File (unauthorized viewing)

cache (unauthorized viewing)

client

Cache (unauthorized viewing)

Proxy server

Network printer

Communication channel (eavesdropping)